**From:** Alan Amesbury
**To:** Microsoft ATR
**Date:** 1/24/02 10:54pm
**Subject:** Microsoft Settlement

There are many aspects of this proposed settlement that bother me. The judgment is putatively in answer to Microsoft (MS) being declared an illegal monopoly. It's my understanding that one of the remedies when dealing with a monopoly is to remedy the problem of others being able to enter the market controlled by the monopoly, yet this proposed settlement doesn't seem to address that. I'm sure this has already been pointed out to you repeatedly, so I'll get to my point.

As a practitioner of computer security for one of the country's largest banks, the mention of security-related items tends to pique my interest the most. In particular, this part of the proposed settlement stood out to me:

> No provision of this Final Judgment shall:
>
>> 1. Require Microsoft to document, disclose or license to third parties: (a) portions of APIs... or layers of Communications Protocols the disclosure of which would compromise the security of a particular installation or group of installations of anti-piracy, anti-virus, software licensing, digital rights management, encryption or authentication systems, including without limitation, keys, authorization tokens or enforcement criteria; or (b) any API, interface or other information related to any Microsoft product if lawfully directed not to do so by a governmental agency of competent jurisdiction.
>>
>> 2. Prevent Microsoft from conditioning any license... related to anti-piracy systems... or third party intellectual property protection mechanisms of any Microsoft product to any person or entity on the requirement that the licensee: (a) has no history of software counterfeiting or piracy or willful violation of intellectual property rights, (b) has a reasonable business need for the API, Documentation or Communications Protocol for a planned or shipping product, (c) meets reasonable, objective standards established by Microsoft for certifying the authenticity and viability of its business, (d) agrees to submit, at its own expense, any computer program using such APIs, Documentation or Communication Protocols to third-party verification, approved by Microsoft, to test for and ensure verification and compliance with Microsoft

specifications.....

As I see it, this section attempts to protect certain security-related functions which, in theory, is a laudable goal. However, it also seems to be a serious loophole. System security is not something that can be trivially separated from the whole, and to attempt to separate it clouds the issue. Consider: if MS develops a communication protocol that is used for authentication (a security function) and file sharing (an information-sharing function), does this settlement give MS the option of not sharing that information?

Consider the Samba project. Samba is a freely available software package that implements MS Windows file sharing on a variety of platforms. It's fast and portable, and reportedly does Windows file sharing better than Windows in some circumstances. Most of Samba's development is done, not by a corporation, but as a hobby by people in their spare time. Because MS didn't disclose its file sharing protocol, Samba was largely developed through reverse-engineering MS protocols.

Because file sharing usually requires some sort of access controls (many times you want to limit who has access to which files), you have to have some sort of user authentication and validation capability built into the software that provides file sharing services. Authentication is clearly a security function. If MS is able to restrict disclosure of security-related protocols, doesn't this hamper the development of competing products that have to rely on MS security protocols in order to interact with MS products?

As for item 2, who decides whether someone has a "reasonable business need" for a security-related API or protocol? Again, the people who developed Samba are a loose-knit group of volunteers. Would volunteers have a "reasonable business need" to obtain access to these protocols under the settlement? It's highly unlikely that MS would determine that they have need, and such volunteers would almost certainly lack the legal resources needed to force MS to turn that information over.

In conclusion, I strongly urge you to *NOT* attempt to separate security factors in the settlement. Security is an integral part of any well-designed API or protocol, and exempting security-related APIs and protocols will very likely provide MS with a loophole that will allow them to perpetuate their monopoly.

Thank you very much for your attention to this matter.

--
Alan Amesbury
security@unregistered.org